## REMARKS

Enclosed is a petition for an extension of time and the appropriate fee.

Claims 1-41 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Jovanovich et al.* ("Jovanovich" U.S. Patent No. 5,703,950) in view of *Matsumoto et al.* ("Matsumoto" U.S. Patent No. 6,286,008). Applicant respectfully traverses this rejection in its entirety.

The present invention as defined in the claims is drawn to a digital content protection system that includes a recording medium apparatus, such as a memory card 200, and an access apparatus, such as a memory card writer 300, for protecting digital content from unauthorized recording and reproduction (Fig. 1 and Specification pages 1 ll. 13-19, 18 ll. 19-24 and 47 ll. 4-5). The digital content protection system operates in an authentication phase and a content transfer phase where the recording medium apparatus and the access apparatus mutually authenticate that the other apparatus is an authorized device prior to transferring encrypted content (Specification page 2 line 20 to page 3 line 7, page 25 ll. 18-27, page 35 line 26 to page 36 line 10, and page 39 ll. 5-19). Therefore, an authorized device does not transfer contents to an unauthorized device, and an unauthorized device cannot transfer contents to an authorized device (Specification page 47 ll. 13-19).

In one embodiment, the authentication phase uses three keys, an inherent key Ki from the recording medium apparatus, an apparatus key Aj from the access apparatus, and a master key Mk that is common to both the recording medium apparatus and the access apparatus (Fig. 9 and Specification page 22 ll. 4-9, page 30 line 26 to page 31 line 15, and page 48 ll. 19-25). The inherent key Ki includes information unique to the recording medium apparatus (Specification page 21 ll. 1-8). The apparatus key Aj includes information unique to the access apparatus (Specification page 30 ll. 14-22). Within the authentication phase, mutual authentication

between the recording medium apparatus and the access apparatus consists of the recording medium being authenticated first to the access apparatus, and then the access apparatus being authenticated to the recording medium apparatus. Once authentication has successfully completed, digital content is either encrypted using the inherent key which is used in the authentication phase and then sent to the recording medium apparatus, or encrypted digital content is received from the recording medium apparatus and decrypted using the secretly transmitted inherent key. This authentication must be successfully concluded before any content is transferred between the recording media apparatus or the access apparatus.

In one embodiment, the recording medium device encrypts its inherent key Ki using a master key Mk to secretly transmit the inherent key to the access apparatus. The access apparatus decrypts the encrypted inherent key to recover the inherent key Ki that has been secretly transmitted. The access apparatus then generates a random number R1 and sends it to the recording medium apparatus. The recording medium apparatus encrypts the random number R1 and sends the encrypted random number S1 to the access apparatus. The access apparatus decrypts the encrypted random number S1 to recover R'1. The original R1 and the recovered R'1 are compared. If they are the same, it confirms to the access apparatus that the recording medium apparatus is authorized. After the recording medium apparatus is authorized, the access apparatus will initiate authentication by secretly transmitting the apparatus key to the recording medium apparatus and proceeding with the authentication of the access apparatus to the recording medium apparatus in a similar manner. With both the recording medium apparatus and the access apparatus authenticating each other, we have a mutual authentication (Figs. 7 and 9, and Specification page 35 line 4 to page 36 line 3, and page 44 line 22 to page 47 line 1). Only after mutual authentication is successfully completed does the digital content protection

system allow the transfer of content encrypted or decrypted with only the inherent key which is used in the authentication phase (Specification page 39 ll. 5-19, page 41 ll. 10-24, and page 47 ll. 10-27).

In the present invention, if a valid apparatus interfaces with an invalid apparatus, the valid apparatus attempts to authenticate the invalid apparatus by initially sending a secretly transmitted inherent key. The invalid apparatus receives the secretly transmitted inherent key and attempts to decrypt and extract the inherent key but cannot do so since the invalid apparatus does not possess the master key with which to decrypt the secretly transmitted inherent key. Since the invalid apparatus does not possess a decrypted version of the secretly transmitted inherent key, the invalid apparatus cannot generate an encrypted version of the random number that is sent to the valid apparatus for decryption and validation of the random number. Hence, authentication of the invalid apparatus to the valid apparatus will fail, and no content data will be subsequently sent to the un-authenticated, invalid apparatus. Thus, it would not be possible to deceive a valid apparatus, or to induce the valid apparatus to transfer data to an invalid apparatus in an unprotected manner.

Jovanovich is drawn to a secure communication system including a host computer and a remote unit. Jovanovich is attempting to solve the problem of providing a flexible retuning of the valid operating frequencies for a radio frequency (RF) device as determined by configuration data while preventing unauthorized retuning by a user (Jovanovich col. 1 ll. 55-56 and col. 2 ll. 10-17). Specifically, Jovanovich is attempting to distribute configuration information to set the operating frequencies based on the supposed locality of operation for the RF device in a way that is not likely to be altered by a user. To achieve this result Jovanovich teaches that the host computer initiates a request for a device ID from the remote unit (Jovanovich Fig. 2 element 41

and col. 4 ll. 29-34). This device ID is an alphanumeric code identifying a particular RF device and is not sent secretly, but rather is sent in an unencrypted condition from the remote device to the host device in reply to the request (Jovanovich col. 4 ll. 4-26). The device ID is loosely verified by reference to a database in the host device that contains records of the particular remote device, and it's purported locality of use (Jovanovich col. 4 ll. 36-41). The device ID is used to encrypt the predetermined configuration information in the host device and decrypt the configuration in the remote device (Jovanovich col. 4 ll. 25-26 and col. 4 ll. 49-53). It is important to note that the device ID is not described in Jovanovich as being sent secretly, or in an encrypted manner. The device ID is the key for encryption and decryption and is sent in the clear from the remote device to the host device. If the cipher algorithm is known, and the key is intercepted, then it is possible to "spoof" or falsify the configuration data and circumvent the security measures described by Jovanovich. The authentication described by Jovanovich only authenticates the remote device to the host device and is a partial, one-sided authentication. There is no description of an authentication of the host device to the remote device. Hence, there is no mutual authentication. However, even though the authentication described in Jovanovich is not mutual, it also diverges from the authentication as claimed in the present invention in that the authentication information of Jovanovich is transmitted openly, not protected, while the present invention includes mutual authentication where the keys used in authentication are secretly transmitted. A secretly transmitted key requires a secondary decryption step prior to extracting the protected key. Further, the present invention describes that the content transmitted in the content transfer phase is encrypted using the inherent key that was sent secretly during the authentication phase. An unauthorized third party can intercept the device ID common key in Jovanovich and possibly recover or falsify configuration information. As claimed in the present

invention, an unauthorized third party cannot access the protected content since they inherent key is secretly transmitted and the protected content will not be sent if mutual authentication does not succeed.

To highlight a difference between Jovanovich and the present invention, according to Claim 1 the inherent information from a first apparatus is secretly transmitted to a second apparatus and the first and second apparatuses perform mutual authentication using the inherent information in order to verify the other apparatus is a valid apparatus. However, Jovanovich teaches sending identifying information that is verified against stored information. In Jovanovich, the authenticity of the sent information is verified, but this process cannot be considered a mutual authentication as described in the claimed authentication phase.

As a consequence of this difference, in Jovanovich an invalid third apparatus can improperly acquire valid identifying information as it is transmitted from a first apparatus to a second apparatus. The invalid third apparatus can then transmit the acquired valid information to the second apparatus. In this case, because what the second apparatus verifies is the only the authenticity of the received information, the second apparatus judges that the received information is valid by checking the received information against stored information. The second apparatus would incorrectly recognize the invalid third apparatus as a valid apparatus and then could transmit secret information to the invalid third apparatus that has been falsely recognized as a valid apparatus. However in the present invention, as the first apparatus secretly transmits the correct inherent information to the second apparatus according to Claim 1, the invalid third apparatus is unable to improperly acquire the secretly transmitted valid inherent information and a mutual authentication cannot be successfully completed. Since authentication is not successfully completed, no subsequent data content is transmitted to the invalid apparatus.

This capability of preventing the transfer of data when mutual authentication has failed is not taught or implied by Jovanovich.

Matsumoto is drawn to a method for accessing digital content where a user already possesses the digital content and an access key is distributed to the user in order to access or utilize the content based on a protocol (Matsumoto col. 1 ll. 6-37 and col. 3 ll. 12-18). Matsumoto teaches that a user possessing the digital content will submit a user ID (UID), a user password (PWu), and a contents ID (CID) to the server without encrypting this essential identifying information (Matsumoto col. 2 ll. 15-20 and 62-64). In another case, Matsumoto teaches the server receives this information and performs a look up of the UID, the PWu, and the CID to generate a decryption key which is returned to the requesting user (Matsumoto col. 2 ll. 27-41). Matsumoto teaches the exchange of random numbers between the user apparatus and the server apparatus for authentication, but in these cases the random numbers are encrypted and decrypted using common information such as the password entered by the user to perform a different type of mutual authentication (Matsumoto col. 3 ll. 21-29). The identifying information related to the user side and the server side can be encrypted and decrypted using a key that is based on the CID or the UID, for example, but that key is not used to encrypt or decrypt the content itself as claimed in the present invention (Matsumoto col. 4 ll. 1-16). The key is merely used to authenticate and gain access to the stored data already in the possession of the user in the form of a CD-ROM containing compressed data, for example (Matsumoto col. 10 line 62 to col. 11 line 4). The key can be used to authenticate and then start a un-compression or restoration program (Matsumoto col. 13 ll. 37-40). It is possible for an unauthorized third party to intercept the content after authentication is completed and access is granted since the data is not necessarily protected after authentication as in the presently claimed invention. In contrast, the

present invention secretly transmits an inherent key that is used to access the protected content itself (Specification page 27 ll. 24-28 and page 37 ll. 14-18).

To highlight a difference between Matsumoto and the present invention, according to Claim 1 the access apparatus encrypts a digital content using the inherent key or decrypts the encrypted digital content using the inherent key that was secretly transmitted in the authentication phase. However, in Matsumoto the user side apparatus simply restores compressed data stored in, for example, a CD-ROM (Matsumoto col. 11 ll. 1-4 and col. 13 ll. 37-40). The key for enciphering/deciphering that is used for the authentication between the user side apparatus and the server side apparatus is not used to perform the above restoration of the compressed data. Since the restored data content is not protected after the type of authentication taught by Matsumoto, it is possible that an invalid third apparatus can intercept the data as it is being restored, and the data content would be compromised to the invalid third apparatus. However, as discussed, in the present invention an invalid third apparatus cannot recover the content data without first successfully completing authentication since the data content will not be sent until after authentication is successfully completed. Hence, even if it was possible that an invalid third apparatus were able to disguise itself as the valid second apparatus and attempt to gain access to the first apparatus after authentication was successfully completed, or if an invalid third apparatus were to intercept the data stream as the data content is transferred, the invalid third apparatus could not successfully decrypt and access the encrypted data content since it does not possess the inherent key.

Claim 1 includes mutual authentication using a secretly transmitted inherent key that is not taught by the cited references in any combination. Further, the cited references do not teach the digital content is encrypted or decrypted by the access apparatus using an inherent key that is

secretly transmitted within a mutual authentication phase as claimed. Applicant respectfully submits that the device ID disclosed by Jovanovich is not equivalent to the inherent key as claimed since the device ID of Jovanovich is not secretly transmitted, can perform limited authentication of only the remote unit to the host computer as discussed above, and does not rely on a secondary decryption for extraction of the inherent key prior to use as is required for a secretly transmitted key. Although the device ID of Jovanovich is used as an encryption and decryption key, it is used in a different way for a different result than that claimed by the present invention. Although a different form of mutual authentication is taught by Matsumoto, Applicant respectfully submits that it is improper to combine the mutual authentication taught by Matsumoto with the partial, one-sided authentication taught by Jovanovich since there is no motivation to combine taught by the references themselves. In Jovanovich, there is no motivation disclosed to authenticate the host computer to the remote unit since the remote unit immediately transmits the device ID used as a key without authentication. The host computer is treated as a trusted host without authentication, and Jovanovich does not suggest any motivation for authentication of the host computer to the remote device. Similarly, Matsumoto does not teach a motivation to combine with Jovanovich since the mutual authentication of Matsumoto does not transfer decryption keys and is limited to unlocking a volume of digital content already possessed by the user. Matsumoto specifically teaches the undesirability of real-time encryption, transmission and decryption of data transmitted from the server (Matsumoto col. 2 ll. 54-64). Applicant respectfully traverse any contention that there is any teaching in either the Jovanovich or the Matsumoto references that would lead a person of ordinary skill in this field to seek such a combination, other than the teaching of the present disclosure. Further, even if the cited

references are combined as suggested, they do not teach all of the claimed elements as described above.

Regarding Claim 2, and in reference to Claim 1 above, Applicant respectfully submits that Jovanovich does not teach the first calculation means using the inherent key nor the first authentication means using the secretly transmitted inherent key since Jovanovich does not teach the remote unit receives a unique information from the host computer and generates an encrypted unique information that is transmitted to the host computer for authentication. The authentication taught by Jovanovich relies on the host computer receiving an unencrypted device ID that can be verified by a lookup in a database of valid device IDs. Further, Claim 2 depends from Independent Claim 1 that is believed allowable as discussed above.

Regarding Claim 3, and in reference to Claim 2 above, Applicant respectfully submits that Matsumoto does not disclose the second calculation means or the second authentication means that uses a secretly transmitted key as claimed. Further, the secret information disclosed by Matsumoto is not the device ID as suggested in the Office Action. In Matsumoto, the device ID is exchanged in an unprotected manner prior to the exchange of the encrypted random numbers which are encrypted using a commonly owned secret key. This common key of Matsumoto is not transmitted and used for decryption as in the present invention. As discussed in regards to the Matsumoto reference above, Matsumoto teaches the random numbers are encrypted and decrypted using common information such as the password entered by the user. Further, Claim 3 depends indirectly from Independent Claim 1 that is believed allowable as discussed above.

Regarding Claims 4, 5, 11 and 12, and in reference to Claim 3 above, Applicant respectfully submits that Jovanovich does not teach the structure of encrypting the device ID (as an inherent key) prior to sending to the host computer. The device ID of Jovanovich is not protected during transmission, and the method described by Jovanovich does not describe secretly transmitting the inherent key as claimed. Although Official Notice was taken that it is well known in the art to encrypt a key when transmitting over a network, Applicant respectfully submits that neither Jovanovich nor Matsumoto teach sending a "secretly transmitted" encrypted key as claimed. As discussed above, Jovanovich teaches sending a device ID in an unprotected manner, and that this unprotected device ID is used as a key. Matsumoto, as discussed above, sends user information in an unprotected manner and then uses a commonly owned key that is not exchanged in order to encrypt and decrypt random numbers. The Office Action suggests that it is inherent that a decryption algorithm must be deployed in order to decrypt data. Applicant respectfully suggests that this assertion highlights a claimed difference between the present invention and the cited references. Specifically, the cited references do not teach encryption of a key, nor exchanging an encrypted key as claimed. As discussed above, Applicant respectfully suggests that the cited references do not teach encryption of an inherent key or exchaing the encrypted inherent key as claimed. Applicant acknowledges that decryption of data necessarily follows encryption of data if the data is to be recovered. Further, dependent Claims 4, 5, 11, and 12 depend indirectly from Claim 1 that is believed allowable.

Regarding Claim 6, an in reference to Claim 5 above, Applicant respectfully disagrees that the device ID of Jovanovich can be interpreted as a secondary encryption or decryption key as claimed in Claim 5. Claim 5 describes the inherent key is encrypted using the first key and

the encrypted first key is decrypted using the second key. Claim 6 identifies the first key and the second key as a single master key, such as Mk as disclosed in the present application (Fig. 9 and Specification page 22 ll. 4-14). Further, dependent Claim 6 depends indirectly from Claim 1 that is believed allowable.

Regarding Claims 7-8, and in reference to Claim 5 above, Applicant respectfully submits that, although public/private key cryptosystems are in wide use, the particular application as claimed is novel over the cited references since the references do not disclose secretly transmitting an inherent key or an apparatus key for use in mutual authentication as discussed above. A particular embodiment for the encryption and decryption of the secretly transmitted keys can include a single master key or a public/private key set. Further, a particular embodiment of extracting the decrypted information can include signature recovery, and does not obviate the novel feature of secretly transmitting the inherent key which is not taught by the references in any combination. Further, dependent Claims 7-8 depend indirectly from Claim 1 that is believed allowable.

Regarding Claims 9-10, and in reference to Claim 4 above, Applicant respectfully submits the use of multiple keys, a key-ring, or sub-keys is an embodiment of the structure defined in Claim 4 regarding the secretly transmitted inherent key which is not taught by the references in any combination. Further, dependent Claims 9-10 depend indirectly from Claim 1 that is believed allowable.

Regarding Claims 13-15, and in reference to Claim 3 above, Applicant respectfully submits that the calculations performed using the inherent key, the transformed inherent key, and the apparatus key are the same as the calculations performed using the secretly transmitted keys

since the operations are performed following authentication where the secretly transmitted keys are transmitted. The multiple device ID storage taught by Jovanovich is the simple look-up table of valid host devices. As discussed, the device ID is loosely verified by reference to a database in the host device that contains records of the particular remote device, and it's purported locality of use (Jovanovich col. 4 ll. 36-41). It is important to note that the device ID is not described in Jovanovich as being sent secretly, or in an encrypted manner as claimed. Further, dependent Claims 13-15 depend indirectly from Claim 1 that is believed allowable.

Regarding Claim 16, and in reference to Claim 14 above, Applicant agrees that the use of random numbers in authentication is desirable to avoid a replay attack, for example, but respectfully submits that the novel use of exchanging separate random numbers encrypted by a resident key and decrypted using a corresponding secretly transmitted key as claimed is not taught by the references in any combination. Matsumoto teaches encyphering/encrypting of random numbers prior to sending the encrypted random number to a receiver (Matsumoto col. 3 ll. 30-44). The presently claimed invention teaches sending random numbers that are encrypted by the receiver and returned to the sender for decryption (Figure 9 and Specification page 44 line 25 to page 47 line 1). Further, dependent Claim 16 depends indirectly from Claim 1 that is believed allowable.

Regarding Claim 17, and in reference to Claim 3 above, Applicant respectfully submits that the cited references do not teach in any combination the decrypting of a first calculated authentication information using a secretly transmitted inherent key as claimed. Further, dependent Claim 17 depends indirectly from Claim 1 that is believed allowable.

Regarding Claim 18 as amended, and in reference to Claim 17 above, Applicant agrees that the use of more than one encryption algorithm may be desirable. However, Claims 17-18 include the novel concept of mutual authentication using a secretly transmitted inherent key and secretly transmitted apparatus key and is not disclosed by the cited references in any combination. Claim 18 recites using a second encryption algorithm, but only within the context of using a secretly transmitted key that is not taught by the references in any combination. Applicant respectfully traverses the assertion in the Office Action that it is well known or inherent that a second decryption algorithm must be used and requests the citation of a reference as to the knowlege and inherency of requiring a second decryption algorithm in this context. Further, dependent Claim 18 depends indirectly from Claim 1 that is believed allowable.

Regarding Claims 19-20, and in reference to Claims 16 and 18 above, Applicant respectfully submits that the use of a subgroup key and a transformed inherent key in the context of a secretly transmitted inherent key for use in mutual authentication is not taught by the references in any combination. Applicant respectfully traverses the assertion the Official Notice that it is well known to encrypt a key when transmitting over a network within this context since Jovanovich does not teach encryption of the device ID. As discussed above, the device ID of Jovanovich is not secretly transmitted as suggested. Applicant respectfully submits that it is improper to combine encryption of the device ID since Jovanovich uses an unencrypted device ID for searching a locally held database in order to validate the device. If the device ID were encrypted, a decryption step would require another key which is not taught or implied by Jovanovich. Hence, Applicant respectfully submits that there is no teaching towards this

combination. Further, dependent Claims 19-20 depend indirectly from Claim 1 that is believed allowable.

Regarding Claims 21-22, and in reference to Claim 3 above, Applicant respectfully submits that encrypting, decrypting, and reproducing protected digital content by using a secretly transmitted inherent key after authentication as claimed is not taught by the references in any combination. The Office Action asserts that Jovanovich "discloses a transfer phase where after successful authentication, access apparatus encrypts a digital content using a secretly transmitted inherent key..." Applicant respectfully traverses this assertion since Jovanovich teaches encryption and decryption using a device ID that is not secretly sent, but rather is sent openly between the remote unit and the host computer (Jovanovich Fig. 2 and col. 4 ll. 46-55). The Office Action asserts that Matsumoto discloses a mutual authentication method where two apparatuses exchange secret information. Applicant respectfully traverses this assertion since the method of Matsumoto teaches a common secret key for encrypting and decrypting random numbers and does not teach the use of a secretly transmitted key for encryption and decryption. As discussed, Applicant respectfully submits that even if the references are combined as suggested, they do not teach all of the claimed elements of the present invention. Further, dependent Claims 21-22 depend indirectly from Claim 1 that is believed allowable.

Regarding Claims 23-31, and in reference to Claim 1 above, Applicant respectfully submits that encrypting and decrypting data blocks using secretly transmitted inherent key or utilizing a file key or a user key for a file of digital content following successfully completion of mutual authentication is not taught by the references in any combination and is not well known in the art. In reference to Claims 16 and 20 above, the use of a seed value to determine a starting

point for a random number generator in combination with the use of the random numbers in mutual authentication as claimed is not taught by the references in any combination. The use of a block cipher is merely one embodiment of encrypting or decrypting content following mutual authentication as claimed which is not taught by the cited references in any combination. Further, Claims 23-31 depend directly or indirectly from Claim 1 that is believed allowable based on the above arguments.

Regarding Claims 32-34, and in reference to Claims 1-3 above, Applicant respectfully submits that a recording medium apparatus embodiment of the digital protection system operating according to the mutual authentication and content transfer phases as claimed is not taught by the cited references in any combination. Since Claims 32-34 are drawn to a particular embodiment of the system recited in Claims 1-3 are believed allowable based on the arguments above.

Regarding Claim 35-37, and in reference to Claims 1-3 above, Applicant respectfully submits that a access apparatus embodiment of the digital protection system operating according to the mutual authentication and content transfer phases as claimed is not taught by the cited references in any combination. Since Claims 35-37 are drawn to a particular embodiment of the system recited in Claims 1-3 are believed allowable based on the arguments above.

Regarding Claims 38-41, and in reference to Claim 1 above, Applicant respectfully submits that an encrypted key generating apparatus embodiment, a digital content protection method embodiment, a digital content protection program embodiment, and computer digital signal embodiment, are each a particular embodiment of the digital protection system operating according to the mutual authentication and content transfer phases as claimed and are not taught

by the cited references in any combination. Since Claims 38-41 are each drawn to a particular embodiment of the system recited in Claim 1, they are believed allowable based on the arguments above.

For at least the reasons stated above, Applicant respectfully requests the rejection of Claims 1-41 be withdrawn.

It is believed that the case is now in condition for allowance, and an early notification of the same is requested.

If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on March 1, 2004.

By: James Lee

Signature

Very truly yours,

**SNELL & WILMER L.L.P.**

Joseph W. Price
Registration No. 25,124
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4920